REMARKS

Claims 1-3, 6, 8, 11, 14, 17, 20-22, 24, 25, and 38-40 are amended. Support for the amendments can be found, for example, in FIGs. 5A, 5B and paragraphs 73-74 of the specification as originally filed. Claims 1-41 remain in the Application. Reconsideration of the pending claims is respectfully requested in view of the above amendments and the following remarks.

I. Claims Rejected Under 35 U.S.C. § 102

A. Claims 1-6, 12-13, 17, 19-22, 24, 26 and 34-40 stand rejected under 35 U.S.C. § 102(b) as being anticipated by U.S. Patent No. 5,953,424 issued to Vogelesang et al. ("Vogelesang"). To anticipate a claim, the Examiner must show that a single reference teaches each of the elements of that claim. Amended Claim 1 recites a cryptographic method, including:

> "generating, at a first entity, a first public key M_B, the first public key M_B being session specific;
>
> receiving, at the first entity, a second public key M_A, the second public key M_A being session specific;
>
> generating, at the first entity, a first session key K_B and a first secret S_B, the first session key K_B being different from the first secret S_B, both the first session key K_B and the first secret S_B being computed from the second public key M_A;
>
> encrypting, at the first entity, a first random nonce N_B with the first session key K_B or the first secret S_B to obtain a first encrypted result;
>
> encrypting, at the first entity, the first encrypted result with the other one of the first session key K_B or the first secret S_B to obtain an encrypted random nonce;
>
> transmitting the encrypted random nonce from the first entity to the second entity;
>
> receiving a response to the encrypted random nonce; and
>
> authenticating through determining whether the response includes a correct modification of the first random nonce N_B" (emphasis added).

Applicants submit that Vogelesang and other cited references do not teach or even suggest each of the elements of amended Claim 1.

Vogelesang discloses a cryptographic system in which signals between two participants are encrypted by a shared secret S. The shared secret S is derived from a public signal (e.g., X) and multiple authentication factors (e.g., K and J). In col. 16, line 26 through col. 17, line 37, Vogelesang describes a sequence of authentication operations, which are cited by the Examiner as anticipating each of the claimed elements. However, Vogelesang does not disclose, in the cited passage or elsewhere in the disclosure, that a random signal transmitted between the two participants is encrypted, first by one of the first session key K_B and the first secret S_B, and then by the other of the first session key K_B and the first secret S_B. In the cited line at col. 16, line 67, Vogelesang at most discloses encrypting two signals with one encryption key (i.e., the shared secret S). There is nothing in Vogelesang that mentions encrypting a random number, in two separate encryption operations, using two different encryption keys that are computed from the same public key.

In the rejection of Claims 14-15, the Examiner cites Bruce Schneier, Applied Cryptography, John Wiley & Sons, 1996, Pages 4-5 and 357 ("Schneier") for disclosing superencrypting in which multiple layers of encryptions are applied. However, Schneier does not disclose using the same public key (e.g., M_A) to compute two different encryption keys (e.g., K_B and S_B) in the disclosed superencrypting. Thus, even assuming for the sake of argument that Vogelesang is combined with Schneier, the cited references do not teach the claimed encryption operations.

Analogous discussions apply to Claims 2-6, 12-13, 17, and 19, which depend from Claim 1 and incorporate the limitations thereof. Analogous discussions also apply to amended independent Claims 20-22, 24, and 38-40, as well as Claims 26 and 34-37, which depend from Claim 24 and incorporate the limitations thereof.

Accordingly, reconsideration and withdrawal of the anticipation rejection of Claims 1-6, 12-13, 17, 19-22, 24, 26 and 34-40 are respectfully requested.

B. Claims 1-2, 6, 8-10, 20-22, and 29-31 stand rejected under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent Application Publication No. 2001/0042205 applied for by Vanstone et al. ("Vanstone").

Vanstone discloses a key establishment protocol which computes a shared key (K) from a public signal (e.g., α^x). However, Vanstone does not disclose using the same public signal (e.g., α^x) to compute two different keys (e.g., K_B and S_B) for use in two separate encryption operations to encrypt a random number. Thus, for at least the foregoing reasons, Vanstone and the other cited references do not teach or suggest each of the elements of amended independent Claims 1, 20-22, 24, and 38-40, as well as their respective dependent claims.

Accordingly, reconsideration and withdrawal of the anticipation rejection of Claims 1-2, 6, 8-10, 20-22, and 29-31 are respectfully requested.

II. Claims Rejected Under 35 U.S.C. § 103(a)

Claims 14-16, 25 and 33 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 5,953,424 issued to Vogelesang et al. ("Vogelesang") in view of Bruce Schneier, Applied Cryptography, John Wiley & Sons, 1996, Pages 4-5 and 357 ("Schneier").

To establish a *prima facie* case of obviousness, the relied upon references must teach or suggest every limitation of the claim such that the invention as a whole would have been obvious at the time the invention was made to one skilled in the art.

Claims 14-16, 25 and 33 depend from their respective base Claims 1 and 24, and incorporate the limitations thereof. Thus, for at least the reasons mentioned above in regard to amended Claim 1, Vogelesang in view of Schneier does not teach or suggest the amended limitations of Claim 1.

Accordingly, reconsideration and withdrawal of the obviousness rejection of Claims 14-16, 25 and 33 are requested.

III. Allowable Subject Matter

Applicants appreciate the Examiner's indication that Claims 7, 18 and 28 would be allowable if rewritten in independent form including all of the limitations of the base claims and any intervening claims. Applicants respectfully submit that the amendments to their base Claims 1 and 24 have obviated the need to rewrite these dependent claims. Thus, for at least the foregoing reasons, Claims 7, 18 and 28 are allowable at least for the reasons mentioned in regard to Claims 1 and 24. Accordingly, reconsideration and withdrawal of the objection of Claims 7, 18 and 28 are requested.

CONCLUSION

In view of the foregoing, it is believed that all claims now are now in condition for allowance and such action is earnestly solicited at the earliest possible date. If there are any additional fees due in connection with the filing of this response, please charge those fees to our Deposit Account No. 02-2666.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP

Dated: July 20, 2006

Thomas Coester

Thomas M. Coester, Reg. No. 39,637

12400 Wilshire Boulevard
Seventh Floor
Los Angeles, California 90025
Telephone (310) 207-3800
Facsimile (310) 820-5988

CERTIFICATE OF FACSIMILE

I hereby certify that this correspondence is being transmitted via facsimile on the date shown below to the United States Patent and Trademark Office.

Amber D Saunders 7/20/06

Amber D. Saunders

Date